



## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<b>(51) International Patent Classification 6 :</b> <b>H04L 9/00</b>	<b>A1</b>	<b>(11) International Publication Number:</b> <b>WO 00/22774</b> <b>(43) International Publication Date:</b> 20 April 2000 (20.04.00)
<b>(21) International Application Number:</b> PCT/US99/24157 <b>(22) International Filing Date:</b> 14 October 1999 (14.10.99) <b>(30) Priority Data:</b> 60/104,270      14 October 1998 (14.10.98)      US <b>(71) Applicant (for all designated States except US):</b> ULTRA INFORMATION SYSTEMS LLC [US/US]; Suite 200, 4984 El Camino Real, Los Altos, CA 94022 (US). <b>(72) Inventor; and</b> <b>(75) Inventor/Applicant (for US only):</b> SPRAGGS, Lynn [CA/CA]; 8604 Kalavista Drive, Vernon, British Columbia V1B 1K3 (CA). <b>(74) Agents:</b> TOCZYCKI, Robert et al.; Carr & Ferrell LLP, Suite 200, 2225 East Bayshore Road, Palo Alto, CA 94303 (US).		<b>(81) Designated States:</b> AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).  <b>Published</b> <i>With international search report.</i>

**(54) Title:** SYSTEM AND METHOD OF AUTHENTICATING A KEY AND TRANSMITTING SECURE DATA

**(57) Abstract**

Authenticating a key of a user is provided by decrypting an encrypted data file provided by the user with a password provided by the user into the authentication key of the user. The encrypted data file can be stored on a RF smart card (106) and can contain encrypted biometric data identifying the user, such as a fingerprint. An additional measure can be used by taking a digitized biometric fingerprint scan (108) of the user and probabilistically comparing the digitized fingerprint scan of the user with the authenticated key of the user (102). The user's key can then be used to securely encrypt and transmit data (110) accordingly knowing that the key has been authenticated.

